Ontologie de l'activité de renseignement

Nicolae Sfetcu

12.02.2019

Sfetcu, Nicolae, « Ontologie de l'activité de renseignement », SetThings (12 février 2019), URL = https://www.setthings.com/fr/ontologie-de-lactivite-de-renseignement/

Email: nicolae@sfetcu.com

Une traduction partielle de :
Sfetcu, Nicolae, « Epistemologia serviciilor de informații », SetThings (4 februarie 2019), MultiMedia Publishing (ed.), DOI: 10.13140/RG.2.2.19751.39849, ISBN 978-606-033-160-5, URL = https://www.setthings.com/ro/e-books/epistemologia-serviciilor-de-informatii/

Dans l'activité de renseignement, le problème ontologique est lié à la nature et aux caractéristiques des entités qui menacent et sont menacées. Selon Eric Little et Galina Rogova, « la menace est un objet ontologique très complexe et, par conséquent, une ontologie appropriée doit être construite conformément aux principes métaphysiques formels qui peuvent prendre en compte la complexité des objets, des attributs, des processus, des événements et des relations qui composent ces états de choses". (Eric G. Little and Rogova 2006)

L'argument de Björn Müller-Wille concernant la sécurité et les menaces permet de mettre en évidence l'interdépendance entre les entités menaçantes et menacées. En ce sens, les analystes de l'information doivent définir à la fois ce qu'est une menace et ce qui est menacé. Ainsi, une

ontologie significative de la menace doit inclure à la fois les menaces et les entités menacées. (Vandepeer 2011)

Développer une ontologie des menaces nécessite une taxonomie. Buzan, Waever et Wilde fournissent une taxonomie potentiellement utile utilisée pour décrire l'analyse de sécurité. (Buzan et al. 1998) Ils soutiennent que l'analyse de la sécurité implique trois acteurs distincts. De cette taxonomie, adaptée à l'analyse du renseignement, résultent les entités suivantes :

- Un *référent* c'est quoi ou qui est menacé ;
- Un *analyste* agit comme un « déterminant de la menace » ; et
- Un *acteur de la menace* qui est évalué par l'analyste comme menaçant le référent.

Le référent de la menace est généralement l'État, à savoir la survie de l'État et de sa population. (Singer 1958) Le *Quadrennial Homeland Security Review* décrit la sécurité comme l'exigence de « protéger les États-Unis et leur peuple, leurs intérêts vitaux et leur mode de vie ». (Department of Homeland Security 2010) La mondialisation rend de plus en plus difficile d'identifier clairement les intérêts de l'État, même de la population. Selon la Convention de Montevedio, les quatre conditions généralement acceptées pour un État sont : une population permanente ; territoire défini ; un gouvernement ; et la capacité d'entrer en relation avec d'autres États. (Australia Department of Defence 2009) Ces exigences se réfèrent généralement à quatre aspects d'un État qui peuvent être menacés, à savoir: la population, le territoire, le gouvernement et les intérêts. Pour la nature et les caractéristiques des menaces étatiques et non étatiques, la manière dont ces entités peuvent menacer ces quatre facteurs est examinée.

Les intérêts de l'État comprennent la menace de l'influence politique de l'État, limitant ainsi la capacité de l'État à développer des relations favorables ou solides avec d'autres États, la stabilité régionale, (a242) la stabilité économique, le développement et l'infrastructure financière de l'État,

(Australia Department of Defence 2009) l'accès aux marchés, les ressources énergétiques, les lignes de communication et la capacité des citoyens à voyager.

Les acteurs non étatiques (en particulier ceux qui menacent) ne sont souvent pas définis. Une définition utile pour les capturer est "... toute personne ou groupe de personnes agissant indépendamment des gouvernements officiels". (Australia Department of Defence 2002)

L'évaluation de la menace (impact) est définie par Steinberg et al comme "le processus d'estimation et d'anticipation des effets sur les situations des actions planifiées ou estimées/anticipées par les participants ; elle comprend les interactions entre les plans d'action de plusieurs acteurs (par ex., en évaluant les susceptibilités et les vulnérabilités aux actions menacées estimées/prévues, en tenant compte de leurs actions prévues)." (Omand 2009) Il s'ensuit que différentes fonctions et éléments d'évaluation des menaces doivent être pris en compte. (Rudd 2008) La complexité ontologique des éléments de menace nécessite une analyse ontologique basée sur la métaphysique, qui peut classer efficacement les différents types d'objets complexes, de propriétés et d'attributs, d'événements, de processus et de relations qui intéressent divers décideurs.

Le traitement de l'évaluation des situations et des menaces (ESM) fait référence à des informations dépendantes du contexte sur les facettes dynamiques de la réalité, (Eric G. Little and Rogova 2006) de sorte que les ontologies de l'ESM doivent être capables de capturer la structure de la réalité en offrant des capacités pour décrire la multitude de types de relations (par exemple, relations spatio-temporelles, intentionnelles et de dépendance) qui existent entre différentes entités situationnelles (et leurs agrégations) à différents niveaux de granularité. (Bittner and Smith 2003) Pour cette raison, les ontologies à utiliser pour évaluer la situation et les menaces nécessitent une compréhension plus large des types de relations et d'entités relationnelles, trouvées initialement dans les écrits d'Aristote (Aristotle 1991) et formalisées plus tard par Edmund Husserl. (Husserl

1900) Il est important que les ontologies ESM soient structurées dans un cadre métaphysique général plus élevé, afin de pouvoir décomposer les éléments les plus abstraits du domaine d'intérêt, ainsi que les relations entre eux.

Eric G. Little et Galina L. Rogova ont développé une "ontologie des menaces", (Eric G. Little and Rogova 2006) une version modifiée de l'ontologie officielle de base (Grenon and Smith 2004) composée de deux sous-niveaux orthogonaux nommés SNAP et SPAN, qui sont conçus pour capturer les caractéristiques spatiales et temporelles de l'ontologie. Sur la base de la distinction entre le continuant et l'occurrence, des objets spatio-temporels ontologiquement complexes ont été modélisés, avec une bifurcation formelle entre les objets en tant qu'éléments pouvant exister entièrement à un moment donné dans l'espace et le temps, par rapport aux événements procéduraux, dont les parties et les relations partielles ont lieu constamment au fil du temps et n'existe donc jamais pleinement dans un lieu ou un moment particulier. Cette distinction a permis d'éviter certains problèmes philosophiques traditionnels d'identité.

L'ontologie officielle de base est conçue selon la théorie de la méréotopologie, (Smith 1996) une théorie qui combine une logique des parties et des relations partielles (par exemple, la méréologie) avec une logique d'expansion spatiale et de connexion (c'est-à-dire la topologie), langage capable de traiter la multitude d'objets ontologiques requis pour le traitement de fusion de niveau supérieur, par exemple, les objets, les propriétés/attributs, les espaces, les temps et les nombreux types de relations simples et complexes qui existent entre eux.

Les informations utilisées dans l'évaluation des menaces sont extrêmement incertaines, avec un bruit de fond, contradictoire, redondant, d'importance variable et de faible fidélité. Il est donc nécessaire d'incorporer l'incertitude, la fiabilité et l'imprécision dans la caractérisation des relations qualitatives méréotopologiques. (Eric G. Little and Rogova 2006)

Au niveau supérieur, dans son ensemble, les gens existent en tant qu'entités relationnelles, et pas seulement en tant que collections d'éléments indépendants. Le problème est ici d'une importance ontologique, où la modélisation des collections d'éléments n'est pas la même que la modélisation de l'ensemble, car le même élément complexe peut être compris différemment selon qu'il est compris comme une collection ou comme un tout. (Smith 1996) La théorie de la méréotopologie fournit un moyen de décrire formellement les types de relations complexes partielles entre eux qui comprennent des éléments tels que les menaces, dans lesquels les trois éléments d'intention, de capacité et d'opportunité sont dans une relation formelle de dépendance fondamentale.

La capture des relations métaphysiques, telles que la dépendance fondamentale, est nécessaire pour concevoir des ontologies de la menace. Compte tenu de la nature complexe des menaces, il est essentiel de concevoir un cadre ontologique pouvant inclure de nombreux types de relations nécessaires à la décomposition correcte des éléments complexes. (E. G. Little and Rogova 2005)

La définition ontologique des certaines caractéristiques essentielles des parties et de leurs relations, ainsi que les métriques et contraintes de proximité, permettront alors une meilleure définition et identification des groupes dispersés.

Une ontologie pour l'analyse et l'action contre les menaces doit être capable de modéliser les distinctions ontologiques entre les menaces potentielles et viables. Cela permet de mieux comprendre comment les éléments de menace (c'est-à-dire les intentions, les capacités et les opportunités) peuvent exister et peuvent évoluer avec le temps. L'escalade des menaces d'un État potentiel à un État viable pourrait être évitée en utilisant des techniques appropriées d'atténuation des menaces.

D'autre part, la stratégie d'amélioration sémantique (AS) (Salmen et al. 2011) est basée sur l'utilisation d'ontologies simples dont les termes sont utilisés pour marquer (ou annoter) les artefacts de données source de manière cohérente. Les termes d'une ontologie AS sont liés ensemble dans une hiérarchie simple par le biais de la relation "is_a" (ou sous-type). Chaque terme n'apparaît qu'une seule fois dans cette hiérarchie et est associé de manière stable aux termes parent et enfant dans la hiérarchie, même si de nouveaux termes sont ajoutés à l'ontologie au fil du temps. Cette stabilité est importante, car le succès de la stratégie nécessite des ontologies qui peuvent être réutilisées à plusieurs reprises pour annoter de nombreux types de données différents de manière à desservir plusieurs communautés autres que les analystes, contribuant ainsi à la création d'une image opérationnelle commune de plus en plus complète. AS est conçu pour être à la fois plus stable et plus flexible que les approches traditionnelles d'harmonisation et d'intégration, qui, généralement basées sur une cartographie *ad hoc* entre les modèles de données, se détériorent souvent au fil du temps. (Smith 2012)

Les ontologies AS sont organisées sur trois niveaux, avec des degrés de flexibilité successifs: 1) Une ontologie unique, petite et neutre du domaine supérieur pour laquelle notre candidat sélectionné est l'ontologie officielle de base; (Volkswagen Foundation 2002) 2) Ontologies de niveau moyen, formées en regroupant des termes qui se réfèrent à des domaines d'action spécifiques ou à des tâches spécifiques, comme l'échange d'informations inter-agences; (Smith, Vizenor, and Schoening 2009) 3) Ontologies de bas niveau qui se concentrent sur des domaines spécifiques. L'approche AS est conçue pour être d'une utilité maximale pour les utilisateurs de l'information. Le contenu ontologique est créé uniquement en réponse aux besoins situationnels identifiés des analystes, et les exigences architecturales sont conçues pour assurer une évolution cohérente des ressources de AS sans sacrifier la flexibilité et l'expressivité

nécessaires au développement réel sur le terrain. (Smith 2012) La stratégie AS peut déterminer le développement ontologique collaboratif et la réutilisation à des fins de collecte de données multiples, à la fois internes et externes.

Bibliographie

Aristotle. 1991. "The Metaphysics." 1991. https://www.amazon.com/Metaphysics-Great-Books-Philosophy/dp/0879756713.

Australia Department of Defence. 2002. "Future Warfighting Concept." http://www.defence.gov.au/publications/fwc.pdf.

Australia Department of Defence, Canberra. 2009. "Defending Australia in the Asia Pacific Century: Force 2030 (2009 Defence White Paper)." Text. 2009. https://www.aph.gov.au/About_Parliament/Parliamentary_Departments/Parliamentary_Library/pubs/rp/rp1516/DefendAust/2009.

Bittner, Thomas, and Barry Smith. 2003. "A Theory of Granular Partitions." In *Foundations of Geographic Information Science*, edited by M. Duckham, M. F. Goodchild, and M. F. Worboys, 117–151. London: Taylor & Francis.

Buzan, Barry, Ole Wæver, Ole Waever, and Jaap de Wilde. 1998. *Security: A New Framework for Analysis*. Lynne Rienner Publishers.

Department of Homeland Security. 2010. "Quadrennial Homeland Security Review Report: A Strategic Frameworkfor a Secure Homeland." https://www.dhs.gov/xlibrary/assets/qhsr_report.pdf.

Grenon, Pierre, and Barry Smith. 2004. "SNAP and SPAN: Towards Dynamic Spatial Ontology." http://ontology.buffalo.edu/smith/articles/SNAP_SPAN.pdf.

Husserl, Edmund. 1900. "Logische Untersuchungen." 1900. https://philpapers.org/rec/HUSLU.

Little, E. G., and G. L. Rogova. 2005. "Ontology Meta-Model for Building a Situational Picture of Catastrophic Events." *2005 7th International Conference on Information Fusion* 1: 8-NaN.

Little, Eric G., and Galina L. Rogova. 2006. "An Ontological Analysis of Threat and Vulnerability." *2006 9th International Conference on Information Fusion*, 1–8. https://doi.org/10.1109/ICIF.2006.301716.

Omand, David. 2009. "TheNationalSecurityStrategy: Implications for the UK Intelligence Community." https://warwick.ac.uk/fac/soc/pais/people/aldrich/vigilant/national_security_strategy1.pdf.

Rudd, Kevin. 2008. "The First National Security Statement to the Australian Parliament, Address by the Prime Minister of Australia." https://dfat.gov.au/people-to-people/public-diplomacy/programs-activities/Pages/speech-by-prime-minister-kevin-rudd-to-the-parliament.aspx.

Salmen, David, Tatiana Malyuta, Alan Hansen, Shaun Cronen, and Barry Smith. 2011. "Integration of Intelligence Data through Semantic Enhancement." In *STIDS*.

Singer, J. David. 1958. "Threat-Perception and the Armament-Tension Dilemma." *The Journal of Conflict Resolution* 2 (1): 90–105. https://www.jstor.org/stable/172848.

Smith, Barry. 1996. “Mereotopology: A Theory of Parts and Boundaries - ScienceDirect.” 1996. https://www.sciencedirect.com/science/article/pii/S0169023X96000158.
———. 2012. “Ontology for the Intelligence Analyst.” 2012. https://philarchive.org.
Smith, Barry, Lowell Vizenor, and James Schoening. 2009. “Universal Core Semantic Layer.” In .
Vandepeer, Charles. 2011. “Rethinking Threat: Intelligence Analysis, Intentions, Capabilities, and the Challenge of Non-State Actors.” Thesis. https://digital.library.adelaide.edu.au/dspace/handle/2440/70732.
Volkswagen Foundation. 2002. “Basic Formal Ontology.” http://basic-formal-ontology.org/.